



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/588,801	06/06/2000	Fred J. Bourgeois III	20570-000100US	9465
20350	7590	01/29/2004	EXAMINER	
TOWNSEND AND TOWNSEND AND CREW, LLP			ZHEN, LI B	
TWO EMBARCADERO CENTER			ART UNIT	
EIGHTH FLOOR			PAPER NUMBER	
SAN FRANCISCO, CA 94111-3834			2126	

DATE MAILED: 01/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/588,801

Applicant(s)

BOURGEOIS, FRED J.

Examiner

Li B. Zhen

Art Unit

2126

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10 November 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-12 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-12 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.
a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1 – 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,289,462 to McNabb in view of U.S. Patent No. 6,052,788 to Wesinger.

As to claims 1 and 5, McNabb teaches the invention substantially as claimed including an operating system [trusted operating system; col. 8, lines 50 – 67] on a computing system [trusted server; col. 8, lines 50 – 67], wherein requests are in the form of encapsulated information [incoming packet, Fig. 5; col. 13, lines 20 – 36], controlling access to actions [controlling access to the processes of a trusted server; col. 60 – 67] and objects [assigning control and access attributes to data objects; col. 5, lines 30 – 46] within the computing system, comprising:

configuring selected domains [compartment or partition] on the computing system as configured domains [portion of the system controlled by the operating system that requires specific access codes to be correlated prior to approving access also referred to as a partition; col. 7, lines 42 – 48], each one of the configured domains comprising a higher-order multidimensional domain space [a security attribute that has been added to all three types of components is the "sensitivity label" 202 or SL...SLs

Art Unit: 2126

can be related in several ways: 1) they can be equal, 2) one can be "greater" (dominates) than another, and 3) they can be "disjoint" (meaning neither is greater than the other); col. 9, lines 5 - 33 and col. 9, line 63 - col. 10, line 11], for segregating system operational functionality according to defined operational boundaries [Multilevel secure...permits access to various sets of information with different sensitivities by users with the correct specific security clearances and needs to know, but that prevents users from obtaining access to information for which they lack authorization; col. 8, lines 15 - 22], the operational boundaries defined by mapping attributes of the requests into individual domains [when a process sends information...the trusted server has modified the OS so that the process's security attributes are attached to the packet...the OS can enforce security on processes based on various security attributes, such as SLs; col. 10, lines 25 - 60];

providing a master daemon [UDE] for selecting the configured domains by utilizing the attributes of the requests [role of the UDE 4 is to examine each incoming request and redirect it to the appropriate service... UDE looks at three factors in making its decision: the ASN applied packet label; col. 11, lines 29 - 39];

instantiating at least one process, instantiating at least one subordinate process [establishing a hierarchy of processes related to a task to be performed by the system in response to a user request; col. 6, lines 1 - 23];

performing at least one other defined action [executing an action associated with the redirected request; col. 5, lines 15 - 30]; and

wherein the subordinate daemons, the subordinate processes, the subordinate threads, and the other defined actions being constrained to operate within one of the configured domains at least as restrictive as the configured domain of the master daemon [separate partition exclusively restricts the available processes and files that may be executed or viewed. The processes are bound by a security mechanism where the services such as http would permit access to only portions of the structure of the computer; col. 18, lines 1 – 15].

As to instantiating at least one subordinate thread, McNabb teaches instantiating a process [col. 6, lines 1 – 23] but does not specifically teaches instantiating thread.

However, Wesinger teaches instantiating a process or thread to handle a request [spawns a process, or execution thread, to create a virtual host VHN to handle that connection request. Each process runs off the same base code; col. 14, lines 38 - 55].

It would have been obvious to a person of ordinarily skilled in the art at the time of the invention to apply the teaching of instantiating a process or thread to handle a request as taught by Wesinger to the invention of McNabb because this will dynamically create a process or thread for each request [col. 14, lines 50 – 54 of Wesinger] and allow multiple requests to be handled simultaneously.

As to claims 2 and 10, McNabb teaches the master daemon controls functionality of all the instantiated daemons [graphic model of the system is modified into a tabular or linked list form that may then be used by the UDE and the security gate 8 to control process activities; col. 21, lines 60 – 67], subordinate daemons, processes, subordinate processes, subordinate threads and the defined actions on selected ones of the

Art Unit: 2126

operating systems on computer systems connected to the network [executing an action associated with the redirected request; col. 5, lines 15 – 30].

As to claims 3 and 11, McNabb teaches the master daemon maintains centralized and coordinated access to subsystems of the computing systems [each event to be performed is handled by one central event controller that comprises each of the aforementioned components (ASN, UDE, Security Gate)...the trusted operating system of the present invention supports SLs and uses them to determine if a user or process can access certain objects or resources; col. 12, lines 33 – 50].

As to claims 4 and 12, McNabb teaches the selected domains are further defined by at least one of a security label [sensitivity label], a set of security labels, a lattice of security labels, a group of security labels, a range of security labels, a combination of collections of security labels, and other defined constructs [processes, files, and other resources that have the same sensitivity label are said to be in the same compartment or partition 11. Programs, data, and network interfaces can be split into separate, isolated partitions with restricted access between them; col. 17, lines 49 – 67].

As to claim 6, McNabb teaches at least one of the computing systems is local [local processor] to the master daemon [means for interpreting requests received whether from the local processor or from remote users that comprises an upgrade/downgrade enforcer to determine accessibility to resources and to direct user requests for data to an appropriate location; col. 11, lines 10 - 39].

As to claims 7 and 8, McNabb teaches at least one of the computing systems is on the network and is remote [remote users] from the master daemon [means for

Art Unit: 2126

interpreting requests received whether from the local processor or from remote users that comprises an upgrade/downgrade enforcer to determine accessibility to resources and to direct user requests for data to an appropriate location; col. 11, lines 10 - 39].

As to claim 9, McNabb teaches the step of causing the master daemon to respond to selected ones of the requests to perform a defined action [executing an action associated with the redirected request; col. 5, lines 15 – 30] on the remote computing system [means for interpreting requests received whether from the local processor or from remote users that comprises an upgrade/downgrade enforcer to determine accessibility to resources; col. 11, lines 10 – 39].

Art Unit: 2126

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 5,845,068 to Winiger teaches a multilevel security port system on a computer operating under a multilevel operating system.

U.S. Patent No. 6,295,605 to Dockter teaches performing multiple levels of security evaluation before certain users can gain access to system resources.


4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Li B. Zhen whose telephone number is (703) 305-3406. The examiner can normally be reached on Mon - Fri, 8:30am - 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Meng-Ai An can be reached on (703) 305-9678. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Li B. Zhen
Examiner
Art Unit 2126

lbz
January 21, 2004


MENG-AI T. AN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100